

The Privacy Report

Issued by Project on Privacy and Data Collection / American Civil Liberties Union Foundation
410 First Street, S.E. ■ Washington, D.C. 20003 ■ (202) 544-2026

Volume II, No. 1, August 1974

SEEING THE FOREST, BUT NOT THE TREES

When Members of Congress discovered last month that American manufacturers planned to display surveillance devices and other crime-fighting hardware at a Moscow trade fair, there was an immediate outcry in both Houses. The Export Administration Act (S. 3792) was up for approval at the time, and the legislators quickly amended it to require the Department of Commerce to draft regulations for the licensing of such sales to Soviet-bloc nations.

Sen. Henry M. Jackson, D-Wash., said the surveillance equipment "could be used to tighten totalitarian control over minorities and dissenting intellectuals." Rep. Charles A. Vanik, D-Ohio, recited passages from Alexander Solzhenitsyn to illustrate how Soviet secret police could punitively deploy lie detectors, laser applications, voice-print devices, night-vision cameras and other sophisticated hardware. In response, Commerce Secretary Frederick B. Dent ruled that licenses would be required for the shipment of any crime control instruments (Export Administration Bulletin No. 119, July 19, 1974), saying the reason for the U.S. concern was "the welfare of persons who seek to exercise their fundamental rights."

Omitted completely was any concern about use of the same made-in-America surveillance devices against American citizens, or the fact that hundreds of millions in unscrutinized taxpayer funds are poured into the research and development, and the dissemination, of the technology of social control. It appears that what is oppressive in the Soviet Union is acceptable here.

The Privacy Project is examining the structure, scope and internal processes of the enormous "surveillance device complex." Within the government, its primary components are the research agencies of the intelligence, military, law enforcement, space and public health communities. Freely interacting with the government, and continually feeding on the hidden flow of federal funds, are an array of large and small corporations, consultants, academic faculties, think tanks and criminal justice units supported by the Law Enforcement Assistance Administration. The entire phenomenon is shrouded in secrecy. Its amorphous form does not readily fit into the jurisdictional boundaries of Congressional oversight committees, and the severe social and political implications of its spectacular growth have never been subjected to rigorous outside assessment.

President Ford will continue to head the Domestic Council Committee on the Right of Privacy. He is scheduled to chair its next meeting in October, and Philip Buchen, one of Ford's closest associates, will continue as executive director, although he was recently named White House counsel. The Committee staff expects to step up its legislative program and still hopes to phase out by early 1975.

IN THE COURTS

Citing sources that vouch for the reliability of the lie detector, the Wisconsin Supreme Court has ruled that polygraph results are admissible in criminal trials if both sides agree (State v. Stanislawski, 62 Wis. 2d. 730, April 2, 1974). A rape defendant had appealed his conviction on the grounds that favorable polygraph results of tests on him and the alleged victim were not admitted. The court laid down strict guidelines for polygraph use, at the discretion of the trial judge, for purposes of corroboration, subject to cross-examination of the examiner. The court relied on State v. Valdez, 91 Ariz. 274, 371 P. 2d. 894 (1962).

Model Code -- The National Association for State Information Systems (P.O. Box 11910, Lexington, Ky. 40511) has drafted a model Information Practices Act for states. It lists criteria for data bank regulations to be devised by a regulatory board and the rights of data subjects.

The ACLU of Southern California has hired a computer systems analyst, Alan Cohen of Xerox Corporation, as a research consultant for privacy litigation and legislation, under a one-year grant from Xerox.

Link-up -- The state of Texas will establish a centralized computer file of the name, Social Security number, race and date of birth of any recipient of state services -- involving rehabilitation, alcoholism, blindness, welfare, mental health, health, education, employment, university and college enrollment, retardation and youth services. Although many federal and state laws governing these programs prohibit such information sharing about recipients, Governor Dolph Briscoe says the index is needed to eliminate duplication in applications and in provision of services. A recipient's consent will be required prior to entry in the system. But the Texas CLU has asked the governor, "What individual who has received services from a mental health clinic, been confined in Texas Youth Council facilities, been treated for alcoholism, or received food stamps would freely consent to having this information float from agency to agency via computer?"

SPN Codes -- The Pentagon claims to have discontinued Separation Program Numbers, the codes on discharge papers that give negative reasons for discharge. However, an internal coding system will be maintained and the military will not replace the coded discharge form unless a serviceperson makes the request. The ACLU and some Congressmen are pressing the Pentagon to eliminate the code totally and provide new forms to all veterans.

QUOTABLE

"As Vice President, I addressed myself to the individual rights of Americans in the area of privacy. There will be no illegal tapings, eavesdropping, buggings or break-ins by my Administration. There will be hot pursuit of tough laws to prevent illegal invasions of privacy in both government and private activities."

President Ford, speech before Congress,
August 12, 1974.

IN THE STATES

At the discretion of the Mental Health Commissioner, attorneys for mental patients, and in some cases patients themselves, have the right to inspect their own records, under a new Massachusetts law (Ch. 348, June 17, 1974) * * * The state of Oklahoma now prohibits any state agency from beginning use of Social Security numbers as identifiers and prohibits the denial of a driver's license for the failure to disclose one's Social Security number (Enr. H.B. 1652, May 3, 1974). * * * A legislative resolution creating an 11-member commission to study unfair compiling of personal data was enacted May 8 in Rhode Island, but no members of the group have yet been appointed and only \$10,000 was appropriated for the group to prepare a report by next April. * * * The confidentiality of school records has been established by law in Wisconsin, effective in September (Ch. 254, Laws of 1973, June 8, 1974). * * * The Dade County Board of Commissioners in Miami has approved a Fair Credit Disclosure Ordinance (74-55) requiring a credit reporting firm to provide a consumer a copy of its report on the individual (including identity of sources); the federal act requires only a verbal description of the report. Credit investigators may knock on neighbors' doors for information now only with permission of the occupant or they will be fined as nuisances. Even stiffer credit provisions are expected to follow in Dade County. * * * Arkansas Attorney General Jim Guy Tucker plans to draft legislation regulating state data banks. * * * The Missouri Division of Health, using its general authority to license hospitals, has begun a mandatory reporting system administered by the Iowa Hospital Association (in Iowa and Wisconsin, as well). For each of its patients, private and public hospitals will have to report admission and discharge date, date of birth, residence (census tract), sex, race, expected source of payment, attending physician, discharge status, services rendered, diagnosis and surgical procedure. Similar data will probably be required in each state as part of the data collection for Professional Standards Review Organizations mandated by federal law.

The Eyes of Texas -- As spokesman for the Citizens Association for Sound Energy in Dallas, Robert Pomeroy was a frequent critic of a proposed nuclear power plant. He spoke out against the plant before the city council in January, and at the First Unitarian Church in March he debated a vice president of Dallas Power & Light. At the time, he was unaware that he was under surveillance by the state Department of Public Safety because of his opposition campaign. At his latest testimony, on July 31, Pomeroy revealed that the DPS was keeping a file on his activities and personal background, and had shared the file with Continental Airlines, for whom Pomeroy works as a pilot. The Pomeroy surveillance turned out to be only one part of a larger DPS investigatory network, that included surveillance of other nuclear power plant opponents in Texas and of the First Unitarian Church, mentioned in the DPS report on Pomeroy as a sponsor of "radical left groups." Pomeroy asked the ACLU of Texas to represent him in a damage suit against DPS; a state senator asked for a legislative investigation of privacy rights of all Texas citizens; and Governor Dolph Briscoe demanded to know whether DPS regularly conducts such surveillance. DPS, admitting that Pomeroy was not suspected of any criminal activity, said it was sorry.

Subscribers who have not already done so are asked to send \$15 (\$5 for students) to defray the costs of publishing The Privacy Report. Contributions to the Privacy Project are tax-deductible and help the project to increase its monitoring of government and private data collection about individuals and to inform citizens of their rights to privacy.

IN CONGRESS

Senator Gaylord Nelson, D -Wis., and Senator Sam J. Ervin, D -N.C., have introduced an amendment to the 1975 appropriations bill for Justice, State, and Commerce that would prohibit funds under the bill (H.R. 15405) to be used for wiretapping in violation of Title III of the Omnibus Crime Control Act of 1968. A vote is expected in late summer. "A stop-gap measure," Ervin called the amendment until Congress legislates with regard to warrant-less "national security" taps. * * * The President has signed the Elementary and Secondary Education Act (H.R. 69) including the "Buckley Amendment" that denies funds to school districts that do not restrict outside access to pupil records and that do not allow parental access. Parents will have the right to inspect experimental instructional materials, and federal evaluators and auditors will still have access to otherwise private pupil data. * * * The government operations committees of both Houses expect to complete mark-up of similar broad-based privacy bills late this month. The Koch-Goldwater proposal in the House, H.R. 14493, and the Ervin proposal in the Senate, S. 3418, would create a federal privacy board to regulate data banks, set privacy standards for data collection, limit use of the Social Security number to Social Security purposes, and perhaps require a privacy impact statement for new computer systems. Currently, the bills exempt criminal investigative files and systems with data that would "seriously damage national defense" if released. * * * The House Republican Task Force on Privacy plans to release a position paper on the issue shortly.

An Alexandria, Va., father tells the following story: "Computers often make mistakes. About two weeks ago, we got a letter from a family in Florida who used to live in Virginia. They had received my daughter's bank statement. The computer made a mistake. Now it wasn't significant because the amount of money was inconsequential; but it might have been if it had been somebody in a different circumstance." The man is Gerald Ford. He called this an example of "the problem of mistaken utilization of private information about you or me or two hundred million others."

Public Opinion -- Four out of five persons questioned think laws are needed to require organizations to notify individuals that personal data is kept on file, get permission before transferring personal information, allow a citizen to challenge his record and to get a copy of it, according to Roper Reports. Two-thirds think legislation is needed to bar demands for the Social Security number where not authorized by existing law; seven out of ten think that giving away or selling mailing lists should be made illegal. The Harris Survey found 75 percent of those polled want further laws to regulate credit reporting practices, although by 69-28 percent, most had not experienced a diminution of privacy because of credit reporting firms.

Tell All -- Thousands of incoming students at more than 200 colleges will be asked to fill out a form next month as part of a continuing survey by UCLA's higher education laboratory. The voluntary survey asks (use only black lead pencil; make no stray markings): parents' income and education, student's name and address, religion, source of expenses, dating practices, self-esteem, political views, ambitions and biases.

A HIDDEN RESOURCE

By Natasha Lisman

When the Civil Liberties Union of Massachusetts began its Project on Privacy and Data Banks a year ago, those concerned about runaway data-gathering were few and their message was either ignored or dismissed. Soon, however, the dam broke, and privacy advocates found themselves at the forefront of a movement spanning a remarkably broad political spectrum and boasting a fair sprinkling of establishment figures.

We decided that our first task was research and self-education. Without gathering information about information-gatherers we could hardly begin to bring legal challenges to their practices or suggest new legal safeguards.

One of the difficulties in acquiring expertise was the lack of resources. Fortunately, we stumbled into what turned out to be a very effective free resource -- state government.

Several months ago, a group of public health planners in charge of a new health information system, called Long Term Care Information System (LTCIS), decided that the system had a potential for invading privacy and that its design should include safeguards. To formulate effective safeguards and to monitor their enforcement, the LTCIS group formed a standing, independent Human Rights Committee, to which they invited public health professionals, lawyers, citizens, and two people from our organization. The Committee's subsequent recommendations have been accepted by LTCIS and also have attracted the attention of the Secretariat of Human Services (the Massachusetts version of the U.S. Department of HEW) as a model for similar rules and regulations for all of the agencies in its jurisdiction.

Such independent committees provide an excellent framework for learning about record-keeping in state government. They have to know what information is collected, on whom, for what purposes, how it is stored, to whom it is disseminated, and how it is used -- precisely the questions any privacy project must address. They contribute the energy, time and expertise of their membership and of an agency staff. And, having an official status in state government, they enjoy an easy access to information about data systems that a private research effort seldom has.

For these reasons, we have eagerly seized every opportunity to serve on or work closely with other similar committees -- the Governor's Commission on Privacy and Personal Data, the Special Legislative Commission on Privacy, the Privacy and Security Council of the Criminal History Systems Board, and the Data Processing Policy Committee of the Department of Mental Health. Not all of these have been as systematic as the LTCIS Committee but, as a general rule, any effort at all is better than none.

We see these committees as more than mere research tools. They represent a vital element in the reform of governmental record-keeping. Legislative reform is often not enough. Laws, often by necessity, tend to be general. To insure their enforcement, we must translate them into more specific rules and regulations. For example, in our bill-drafting experience, we have often found it impossible to go beyond the generality that agencies should restrict their data gathering to only that information which they

(continued on page 6)

(continued from page 5)

need to fulfill their legal duties. Lest this "need to know" principle remain an unenforceable piety, however, it must be complemented by an administrative rule based on what a particular agency actually needs. Thus, if it turns out that agency "X" makes decisions about people not at the central level but only at the level of its field offices, and that it needs information at the top only for statistical purposes, it should promulgate a rule against centralization of records in any but anonymous form. It is in the formulation of such rules that the chief value of privacy committees lies.

It should be kept in mind, however, that advisory committees are pluralistic bodies -- the conclusions they reach are results of compromise and do not always measure up to the strictest standards. Using the material accumulated by a committee, a group can proceed to fill any gaps through some other means. We have not, for example, succeeded in persuading some committees to accept our views. But we have learned what the laws are, where records are, and what the prevailing attitudes of record-keepers are -- useful knowledge for any future education campaigns or litigation.

A committee also must keep its recommendations within the existing legal limits. It may not forbid an obnoxious data-gathering practice, for instance, if this practice is mandated by an equally obnoxious law. While the committee can not challenge the law in the courts, a public interest group can, again, build its case in part on the facts the committee has gathered.

Getting a committee created in state government should not be difficult. Government officials, after all, generally love study committees -- too often because it is the most meaningless response to a problem. In the area of privacy, however, studies are badly needed and a public interest group can do a good deal to make sure they are followed by deeds.

Natasha Lisman is director of the Project on Privacy and Data Banks of the Civil Liberties Union of Massachusetts.

THE PRIVACY REPORT is published monthly by the Project on Privacy and Data Collection of the American Civil Liberties Union Foundation. For a subscription (\$15 a year, \$5 for students) write: Privacy Project, 410 First Street S.E., Washington, D.C. 20003 or phone (202) 544-2026. The Privacy Project is a non-profit, tax-exempt effort to monitor increased data collection by state, local and federal governments, as well as by private institutions, and its impact on the individual's right to privacy. Tax deductible contributions aid the work of the project. Checks should be made payable to Privacy Project. DOUGLASS LEA, Director; ROBERT E. SMITH, Associate Director; SHARON E. BIEDERMAN, Administrative Assistant

Privacy Project
410 First Street S.E.
Washington, D.C. 20003